

Daniel J. Stephenson (SBN 270722)  
Dan.Stephenson@klgates.com  
K&L GATES LLP  
10100 Santa Monica Boulevard  
Seventh Floor  
Los Angeles, CA 90067  
Telephone: +1 310 552 5000  
Facsimile: +1 310 552 5001  
  
Attorneys for Defendant  
Lenovo (United States), Inc.

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA  
SAN JOSE DIVISION

IN RE: LENOVO ADWARE LITIGATION,

Case No. 15-md-02624-RMW

This Document Relates To: All Actions

**LENOVO'S RESPONSE TO MOTIONS  
FOR APPOINTMENT OF INTERIM LEAD  
COUNSEL**

Date: July 17, 2015  
Time: 9:00 a.m.  
Judge: Ronald M. Whyte  
Courtroom: 6, 4th Floor

**INTRODUCTION**

This is not a typical cybersecurity case. In a typical cybersecurity case, a large corporation or government agency has its information systems “hacked” by a criminal, who thereby takes possession of the personal and financial data of millions of persons. In the case at hand, by contrast, individual laptop owners may have experienced a temporary increase in hacking risk, but they weren’t actually hacked. Nor were users’ personal or financial information “intercepted” by anyone, and certainly not by Lenovo. While the Superfish software had issues, little if any harm was done.

The challenge faced by counsel and the Court in this case is to efficiently resolve a low-damages dispute. The facts are not complicated and what happened has been well-publicized. In analyzing the petitions of the candidates for lead counsel, the guiding star should not be who can handle the biggest, most complex cases. It should be who can best streamline and reduce litigation cost.

Lenovo (United States), Inc. (“Lenovo”) agrees that interim lead counsel should be appointed, and has no preference among the highly qualified firms who have submitted lead counsel petitions. Lenovo submits this Response to clarify certain factual statements in the various submissions.

### UNDERLYING EVENTS

Four Motions for appointment of lead counsel (“Motions”) have been submitted, and all of them give brief descriptions of the underlying facts. Lenovo submits that certain facts merit clarification.

First, the Superfish Visual Discovery program (the “Software”) did not collect, receive, monitor, or intercept any personal, financial, or health information of any user at any time. The program “did not log users’ keystrokes, did not send Superfish users’ user names, email addresses, passwords, or other personally identifiable information, nor did Superfish receive, collect, or store such information.” (Ex. A, Daniel Decl. ¶ 4.) As the Software does not transmit personal information, Lenovo did not receive or store any such information either. (Ex. B, Grant Decl. ¶ 3.)

Second, in the fall of 2014, Superfish designed a new version of the Software, Version 1.0.0.5. (Ex. B, Grant Decl. ¶ 5.) Unlike the original version, Version 1.0.0.5 did not use a self-signed root certificate with a private key stored on the device. (Id.) Thus, any user with Superfish Version 1.0.0.5 on his or her device did not face the security vulnerability posed by the original version.

Third, when Lenovo discovered the security deficiency in late February 2015, it took swift and decisive action to remove the Superfish Software from all affected computers. Specifically, Lenovo:

1. Issued public statements, website notices, links on Twitter, gave media interviews, and otherwise informed the public and users about the need to remove the Software.
2. Developed and provided a free uninstall program to remove the Software and all remnants/certificates.
3. Worked with leading anti-virus program vendor McAfee to remove the Software completely. Lenovo IdeaPad laptops are shipped with a trial version of McAfee; Lenovo also offered a free 6-month subscription or extension of the McAfee anti-virus program.
4. Worked with Microsoft to remove the Software via Windows Defender, a free program that launches when no other anti-virus software is operating.

5. Worked with Symantec, the maker of Norton AntiVirus, another leading anti-virus program, to add the Software removal to Symantec's functionality.

6. Issued a Security Message to users directly via the Lenovo Messenger advisory tool pre-installed on every affected computer. The message went out on March 21, 2015 to users whose computers still contained the Software. The message included instructions on how to manually or automatically remove the Software. (Ex. C, Hunt Decl. ¶ 3.)

By the end of March, the Superfish Software had already been removed from at least 80-90% of the affected computers, and systems were in place to eliminate the rest. (Ex. C, Hunt Decl. ¶¶ 3-4.)

Fourth, none of the named Plaintiffs represented in the Motions allege that they were "hacked" as a result of having the Superfish Visual Discovery program. Such a hacking would have required the following to occur simultaneously:

1. The user had the original version of the Software installed on his or her computer;
2. The user had not uninstalled the program, inactivated it, or had it eliminated automatically by an antivirus program;
3. The user was connected to the internet;
4. The user was connected via an open, unsecured network (like a coffee shop);
5. A hacker with criminal intent was present at the same place and time;
6. The hacker knew that the computer in question had the Superfish Software onboard;
7. The hacker knew how to exploit Superfish, or had the time and patience to guess the password by trial and error; and
8. The hacker felt it was worth his or her time, and the risk of criminal prosecution, to hack a single person's computer for the limited information available.

Given the perfect storm of circumstances that must be present, the absence of hacking events is to be expected. Even in cases where an individual is actually hacked, the "average identity fraud victim incurred a mean of \$365 in costs as a result of the fraud." (*Wood* PI Mem. at 12.) For all these reasons, Lenovo submits that this is a small-damages case.<sup>1</sup>

---

<sup>1</sup> In light of this, statements to the effect that Lenovo is more financially viable than Superfish are irrelevant. It is also worth noting that Lenovo received no revenues from having installed the Superfish program. In fact, the installation has cost Lenovo significantly.

## PROGRESS OF THE CASE TO DATE

All four of the Movants contend that they have extensively investigated the case and have moved it forward in one way or another. Lenovo agrees that none of the firms have been sitting on their hands. Without showing a preference for any firm over another, Lenovo wishes to clarify some of the statements made on this subject.

One of the groups asserts that it has advanced plaintiffs' interests the furthest because it brought a Preliminary Injunction motion (the "PI Motion"). Lenovo believes that the PI Motion accomplished nothing. The PI Motion was filed in early March and asserted that users faced imminent harm. Lenovo showed that there was and is no imminent harm for the reasons outlined above. Chief Judge Dever in the Eastern District of North Carolina did not rule on the PI Motion, which has now been pending for over four months. It would be fair to assume that had the Court seen an imminent danger, there would have been at least a hearing. Nor did the plaintiffs in any of the other 27 cases see an imminent danger – no one else filed such a motion. The filing of the PI Motion, rather than establishing advancement, shows that without tight control, wasteful activity can quickly and unnecessarily eat up resources in a small-damages case.

The same group asserts that the PI Motion was the impetus for Lenovo sending the Lenovo Messenger security message on March 21. That is not the case. The March 21 launch was in the works before the Preliminary Injunction motion was filed. It is also inaccurate to suggest that the PI Motion forced Lenovo to make admissions that it otherwise would not have made. In reality, almost everything about the Lenovo-Superfish saga was extensively documented in the public sphere, and the "admissions" were defense-positive facts that undercut the plaintiffs' Preliminary Injunction argument.

Some of the Motions refer to contacts between counsel for plaintiffs and counsel for Lenovo. For the sake of clarity, Lenovo offers the following regarding its contacts with Plaintiffs' counsel:

1. Lenovo's counsel has had numerous productive telephone conversations and email communications with the Pritzker Levine firm.

2. Lenovo's counsel has had a one-hour meeting, several telephone conversations and email correspondence with the Robbins Geller and Edelson firms.

3. Lenovo's counsel has had several cordial conversations with the Block Leviton and Van Laningham Duncan firms, much of which related to the PI Motion. Obviously, the parties did not see eye-to-eye on the PI Motion, but the relationship was cooperative and the communications productive.

4. Lenovo's counsel has had no personal communications with the Saveri firm, but has no reason to believe that a relationship with that firm would be anything other than cooperative.

5. Lenovo stated an interest in an early mediation and engaged in discussions toward that end, primarily with the Robbins Geller and Edelson firms. When Lenovo discovered that there was disagreement among the plaintiffs about early mediation, it decided to wait for consensus on the plaintiff side. Lenovo engaged in productive discussions on such topics as the role of Lenovo Group, Ltd., evidence preservation and ESI, but no agreements were reached.

### ASSERTED CLAIMS

The discovery of the security vulnerability in the Superfish Software triggered the filing of 28 essentially duplicative lawsuits. Each suit is a purported nationwide class action. The claims are similar from suit to suit. The filings are a classic example of overkill.

The plethora of claims also illustrates overkill. More than 30 causes of action have been alleged, from breach of warranty to RICO, violation of federal wiretap laws, conspiracy, and state law claims of various genres. Some of the Movants suggest that bringing far-reaching claims (like RICO) shows their creativity and aggressiveness. However, Lenovo submits that what is called for here is the ability to boil the case down to the heart of the matter rather than adding more layers. The assertion of more than 30 claims, if that carries forward into the Consolidated Amended Complaint, will lead to extensive motion practice as most of the claims are tenuous at best.<sup>2</sup>

---

<sup>2</sup> Indeed, all of the claims will face a formidable hurdle on the issue of standing. *Clapper v. Amnesty Int'l USA*, 568 U.S. \_\_\_, 133 S. Ct. 1138, 1147 (2013) (holding that increased security risk is too speculative to support the plaintiff's standing); *Katz v. Pershing*, 672 F.3d 64, 79-80 (1st Cir. 2012) (plaintiff lacked standing to assert consumer protection claims based on increased risk of a future security breach). The "wiretapping" claims against Lenovo are untenable because Lenovo did not monitor, receive, store, or intercept the content of any communications. *In re Carrier IQ, Inc. Consumer Privacy Litig.*, 2015 U.S. Dist. LEXIS 7123, \*103-04 (N.D. Cal. Jan. 21, 2015) (where software installed on smartphones allegedly collected consumer data, device manufacturers were dismissed because plaintiffs could not allege "that any device manufacturer actually received copies of the plaintiffs' text messages or internet search inquiries"). The racketeering claims here are simply beyond the pale.

Three of the four Motions look to appoint interim “class” counsel, and the fourth seeks appointment of “lead” counsel that will protect class interests. While Lenovo agrees that lead counsel should be appointed, Lenovo does not assume that a class will, or should, be certified here. Indeed, the largest single issue will be damage (if any) to users, which will be a predominantly individualized inquiry. There are several other individual issues identified in the Motions: (a) some people bought directly from Lenovo while others bought from retailers with potentially different contractual provisions; (b) some people had the original version of Superfish while others had the later, more secure version; (c) the Superfish Visual Discovery program had an opt-out screen that some users clicked on while others elected to proceed; (d) all users had the ability to uninstall the program from the beginning, and some did; (e) some users do not connect to the Internet; and (f) purchasers who bought after a certain date had a version of McAfee antivirus software onboard that would have automatically removed the Superfish program on first boot. These are just the tip of the iceberg in terms of potential individual issues.

The bottom line is that this may or may not be a class action and the skills required of lead counsel will mostly involve efficiency – boiling the case down instead of inflating it up.

### CONCLUSION

Lenovo reiterates that it has no preference among Movants and is confident it can work cooperatively with any of the candidate firms. The guiding principle should be that this is a low-damages case, so that cost reduction and simplification are the preferred skills.

Respectfully submitted,

K&L GATES LLP

Dated: July 7, 2015

By: /s/ Daniel J. Stephenson

Daniel J. Stephenson

Attorneys for Defendant  
Lenovo (United States), Inc.

**CERTIFICATE OF SERVICE**

The undersigned hereby certifies that on the 7th day of July, 2015, a true and correct copy of the foregoing document: **LENOVO'S RESPONSE TO MOTIONS FOR APPOINTMENT OF INTERIM LEAD COUNSEL** was served on all counsel of record who have consented to electronic service via the Court's CM/ECF system. Any other counsel of record who have not registered as an ECF user will be served by facsimile transmission or first class mail.

/s/Daniel J. Stephenson  
Daniel J. Stephenson